(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 41 00 151 A 1**

(51) Int. Cl.[5]:
G 07 F 7/12
G 06 F 11/28
G 11 C 29/00

(21) Aktenzeichen: P 41 00 151.6
(22) Anmeldetag: 4. 1. 91
(43) Offenlegungstag: 19. 12. 91

DE 41 00 151 A 1

(30) Unionspriorität: (32) (33) (31)
15.06.90 JP 2-157845

(71) Anmelder:
Mitsubishi Denki K.K., Tokio/Tokyo, JP

(74) Vertreter:
von Bezold, D., Dr.rer.nat.; Schütz, P., Dipl.-Ing.; Heusler, W., Dipl.-Ing., Pat.-Anwälte, 8000 München

(72) Erfinder:
Yamaguchi, Atsuo, Itami, JP

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) IC-Karte

(57) Die IC-Karte mit einem in ihr enthaltenen Produkt-Testprogramm wird mit einem Lesespeicher versehen. Dieser Lesespeicher speichert verschiedene Unterprogramme und ist so ausgebildet, daß wenn ein der betreffenden IC-Karte individuell zugeordneter Geheimcode bereits in einem nichtflüchtigen Speicher der IC-Karte gespeichert worden ist, ein von außen eingegebener Geheimcode mit dem gespeicherten Geheimcode verglichen wird und wenn der Vergleich positiv ausfällt, wird der nichtflüchtige Speicher initialisiert. Das Testprogramm kann erst ausgeführt werden, nachdem die Initialisierung fertig ist.

DE 41 00 151 A 1

Beschreibung

Die vorliegende Erfindung betrifft eine IC-Karte, insbesondere eine IC-Karte, welche sowohl ein Testprogramm zum Prüfen der IC-Karte selbst als auch ein Anwendungsprogramm zum Durchführen verschiedener gewünschter Funktionen der IC-Karte enthält.

Ein in einer IC-Karte selbst gespeichertes Testprogramm ist ein Programm zum Durchführen von Prüfungen im wesentlichen aller Funktionen der IC-Karte, und es kann daher auf jede gewünschte Adresse in den Speichern der IC-Karte zugreifen. Um zu verhindern, daß andere Programme, die in der IC-Karte gespeichert sind, durch das Testprogramm unbefugt gelesen und kopiert oder zerstört werden können, muß bei der Ausführung des Testprogramms ein hoher Grad von Sicherheit gewährleistet sein.

Zur Erläuterung der diesbezüglichen Probleme sei auf **Fig. 1** verwiesen, die ein vereinfachtes Prinzip-Blockschaltbild einer IC-Karte **10** zeigt. Die IC-Karte **10** enthält eine zentrale Prozessoreinheit (CPU) **1** zur Durchführung und Steuerung verschiedener Programme und einen System-Lesespeicher (ROM) **3**, in dem ein Testprogramm für verschiedene Funktionsprüfungen des Produkts oder der IC-Karte im Verlaufe ihrer Herstellung gespeichert ist. Die IC-Karte enthält ferner ein Anwendungs-ROM **4**, welches ein Anwendungssprogramm zur Durchführung verschiedener Funktionen speichert, die der IC-Karte zugeordnet sind, weiterhin einen nichtflüchtigen, elektrisch löschbaren und programmierbaren Lesespeicher (EEPROM) **5**, in dem ein geheimer Code, der ausschließlich der betreffenden IC-Karte zugeordnet ist und den Typ dieser IC-Karte bezeichnet, ein Speicherungs-Verifizierungscode, der anzeigt, daß der geheime Code der gespeichert worden ist, persönliche Information eines Benutzers der Karte usw. eingeschrieben und gespeichert sind, und einen Speicher mit wahlfreiem Zugriff (RAM) **6** zur zeitweiligen Speicherung von Daten. Diese Komponenten **1** bis **6** sind miteinander durch einen System-Bus **2** gekoppelt. Die Karte weist ferner mehrere Anschlüsse auf: Einen Anschluß **P1** für eine positive Versorgungsspannung, einen Masse-Versorgungsspannungsanschluß **P2**, einen Rückstellsignaleingangsanschluß **P3**, dem ein Rückstellsignal zur Initialisierung der CPU **1** zuführbar ist, einen Taktsignaleingang **P4**, dem ein Taktsignal zuführbar ist, und einen I/O-Anschluß **P5**, mit dem eine Eingangs-Ausgangs-Schaltung **7** gekoppelt ist, die ihrerseits ebenfalls an den System-Bus angeschlossen ist, um Daten über den I/O-Anschluß **P5** zwischen der IC-Karte **10** und einer nicht dargestellten äußeren Einrichtung übertragen zu können.

Fig. 2 zeigt ein konventionelles IC-Kartensystem, anhand dessen die in **Fig. 1** dargestellte IC-Karte **10** genauer erläutert werden soll. Wie erwähnt, speichert das System-ROM **3** ein Testprogramm **31**, mit dem der Hersteller der IC-Karte verschiedene Funktionen und Operationen der IC-Karte während der Herstellung prüfen kann, ein Verzweigungsunterprogramm **32**, welches entscheidet, ob das Testprogramm **31** oder ein im Anwendungs-ROM **4** gespeichertes Anwendungsprogramm **41** durchgeführt werden soll und welches eine Verzweigung auf das durchzuführende Programm bewirkt; ein Speicherungs-Verifizierungs-Unterprogramm **34** zum Verifizieren, daß ein geheimer Code, der der betreffenden IC-Karte exklusiv zugeordnet ist, im EEPROM **5** gespeichert worden ist und ein Geheimcode-Verifizierungs-Unterprogramm **35** zum Verifizieren,

daß ein von außen über den I/O-Anschluß **5** eingegebener geheimer Code und der früher schon im EEPROM **5** gespeicherte geheime Code übereinstimmen. Das Anwendungs-ROM **4** speichert das Anwendungsprogramm **41**, welches dazu dient, die verschiedenen, vom Benutzer der Karte gewünschten Funktionen durchzuführen, wie bereits oben erwähnt wurde. Nach dem Abschluß des Herstellungsprozesses der IC-Karte wird ein Geheimcode **51**, der der betreffenden IC-Karte exklusiv zugeordnet ist, in das EEPROM **5** geschrieben und in diesem gespeichert. Außerdem wird ein getrennter Speicherungs-Verifizierungscode **52** zum Verifizieren, daß der der betreffenden IC-Karte zugeordnete Geheimcode eingeschrieben und gespeichert worden ist, in das EEPROM **5** eingeschrieben und in diesem gespeichert. Aufgrund dieses Speicherungs-Verifizierungscodes **52** läßt sich feststellen, ob der individuelle Geheimcode **51** gespeichert worden ist oder nicht. Das Bitmuster des Speicherungs-Verifizierungs-Code **52** ist so gewählt, daß es weder mit irgendeinem Bitmuster der Anfangswerte im EEPROM **5** noch mit irgendwelchen Bitmustern, die später in das EEPROM **5** eingegeben werden können, übereinstimmt.

Wenn dem Rückstellsignalanschluß **P3** der Anordnung gemäß **Fig. 2** ein Rückstellsignal zugeführt wird, liest die CPU **1** eine Anfangsadresse des Verzweigungsunterprogrammes **32**, die an einer bestimmten Adresse im System-ROM **3** gespeichert ist, und beginnt die Ausführung des Verzweigungsunterprogramms an der herausgelesenen Adresse. Im Verzweigungsunterprogramm **32** wird das Speicherungs-Verifizierungs-Unterprogramm **34** ausgeführt, wenn dem I/O-Anschluß **5** ein Kommando zur Ausführung des Testprogramms **31** von außen zugeführt wurde. Im Speicherungs-Verifizierungs-Unterprogramm **34** wird auf der Basis des im EEPROM gespeicherten Speicherungs-Verifizierungs-Code **52** festgestellt, ob der Geheimcode **51** in das EEPROM **5** eingeschrieben worden ist oder nicht. Wenn der Geheimcode schon eingeschrieben worden ist, wird das Geheimcode-Verifizierungs-Unterprogramm **35** ausgeführt. Wenn andererseits der Geheimcode noch nicht im EEPROM **5** gespeichert worden ist, erfolgt keine Verifizierung des Geheimcodes, sondern es wird sofort das Testprogramm **31** durchgeführt. Wenn der Geheimcode **51** bereits gespeichert worden war, wird er mit dem über den I/O-Anschluß **P5** eingegebenen Geheimcode verglichen. Nur wenn diese Code übereinstimmen, wird das Testprogramm **31** durchgeführt, wenn nicht, wird der Betrieb beendet. Dieser Stand der Technik hat also den Vorteil, daß verschiedene Geheimcode für die jeweiligen Karten verwendet werden können, da der Geheimcode in einem EEPROM gespeichert wird.

Persönliche Informationen, die in IC-Karten des oben erwähnten Typs gespeichert sind, können unter Verwendung des Testprogramms gelesen oder geändert werden. Insbesondere kann der Inhalt des EEPROMs **5** durch eine Person, die den der betreffenden IC-Karte zugeordneten Geheimcode weiß oder zufällig dessen Kenntnis erlangt, unbefugt herausgelesen und kopiert oder geändert werden.

Aus der JA-OS 62-2 11 765 ist eine IC-Karte bekannt, bei der alle in einem Datenspeicher gespeicherten Daten gelöscht und dadurch ihre Kenntnis verhindert wird, wenn ein der betreffenden Karte exklusiv zugeordneter und in ihr eingeschriebener und gespeicherter Geheimcode mit einem von außen eingegebenen Geheimcode übereinstimmt. Diese IC-Karte kann jedoch nicht durch

BNSDOCID: <DE___4100151A1_I_>

ein Testprogramm hinsichtlich verschiedener Merkmale geprüft werden, bevor der Geheimcode der Karte gespeichert worden ist.

Der vorliegenden Erfindung liegt dementsprechend die Aufgabe zugrunde, eine IC-Karte anzugeben, bei der es selbst wenn irgendjemand bewußt oder zufällig Kenntnis von dem der betreffenden Karte exklusiv zugeordneten Geheimcode erlangt hat, unmöglich ist, irgendwelche Daten, die sich auf den Karteninhaber beziehen, aus dem EEPROM 5 herauszulesen, während es andererseits möglich ist, die IC-Karte hinsichtlich verschiedener Merkmale unter Verwendung eines Testprogramms ungehindert zu testen, bevor der exklusive Geheimcode in die Karte eingespeichert worden ist.

Die erfindungsgemäße IC-Karte enthält eine nichtflüchtige Speicheranordnung, in der Daten gespeichert werden können. In dieser nichtflüchtigen Speicheranordnung wird ein Geheimcode, der von Karte zu Karte verschieden ist, gespeichert. Der Geheimcode dient beispielsweise zur Identifizierung des Kartentyps. Ferner wird in der nichtflüchtigen Speicheranordnung ein Speicherungs-Verifizierungs-Code gespeichert, um zu verifizieren, daß der Geheimcode bereits gespeichert worden ist. Die IC-Karte enthält ferner eine erste Lesespeicher- oder ROM-Anordnung, die ein Anwendungsprogramm zur Durchführung gewünschter Funktionen der IC-Karte speichert, eine zweite ROM-Anordnung, die ein Testprogramm sowie ein Verzweigungsunterprogramm, ein Speicherungs-Verifizierungs-Unterprogramm, ein Geheimcode-Verifizierungs-Unterprogramm und ein Initialisierungs-Unterprogramm speichert. Das Verzweigungsunterprogramm dient dazu, festzustellen, ob das Testprogramm oder das Anwendungsprogramm auszuführen sind. Wenn festgestellt wird, daß das Testprogramm auszuführen ist, stellt das Speicherungs-Verifizierungs-Unterprogramm dann aufgrund des Speicherungs-Verifizierungs-Code in der nichtflüchtigen Speicheranordnung vor der Ausführung des Testprogramms fest, ob der Geheimcode bereits gespeichert worden ist oder nicht. Wenn das Speicherungs-Verifizierungs-Unterprogramm feststellt, daß der Geheimcode bereits gespeichert worden ist, vergleicht es den von außen in die Karte eingegebenen Geheimcode mit dem Geheimcode in der nichtflüchtigen Speicheranordnung. Wenn das Geheimcode-Verifizierungs-Unterprogramm feststellt, daß der von außen eingegebene Geheimcode mit dem in der nichtflüchtigen Speicheranordnung gespeicherten Geheimcode übereinstimmt, initialisiert das Initialisierungs-Unterprogramm die nichtflüchtige Speicheranordnung und ermöglicht die Durchführung des Testprogramms erst nach der Beendigung der Initialisierung. Die IC-Karte enthält ferner eine Steuereinrichtung zum Ausführen und Steuern der jeweiligen Programme, Eingang/Ausgang-Steuereinrichtungen zum Steuern der Signal-Eingabe und -Ausgabe von einer äußeren Einrichtung bzw. in diese und einen System-Bus zur Signalübertragung zwischen den verschiedenen Einrichtungen. Zur Durchführung des Testprogramms, wenn ein der betreffenden IC-Karte exklusiv zugeordneter Geheimcode bereits in die nichtflüchtige Speicheranordnung eingeschrieben worden ist, wird ein von außen eingegebener Geheimcode verifiziert und die nichtflüchtige Speicheranordnung wird initialisiert und dann erst kann das Testprogramm durchgeführt werden. Wenn die nichtflüchtige Speicheranordnung andererseits keinen Geheimcode für die betreffende Karte enthält, kann das Testprogramm ohne Initialisierung der nichtflüchtigen Speicheranordnung durchgeführt werden.

Im folgenden wird ein Ausführungsbeispiel der Erfindung unter Bezugnahme auf die Zeichnungen näher erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung des prinzipiellen Aufbaus einer IC-Karte;

Fig. 2 ein Flußdiagramm zur Erläuterung der Arbeitsweise einer bekannten IC-Karte; und

Fig. 3 ein Flußdiagramm zur Erläuterung der Arbeitsweise einer IC-Karte gemäß einer bevorzugten Ausführungsform der Erfindung.

Eine bevorzugte Ausführungsform einer IC-Karte gemäß der Erfindung soll nun unter Bezugnahme auf die **Fig.** 1 und 3 näher erläutert werden. Die generelle Konstruktion der erfindungsgemäßen IC-Karte entspricht im wesentlichen der in **Fig.** 1 gezeigten Blockdarstellung, auf die bereits oben Bezug genommen worden ist.

Fig. 3 ist ein Flußdiagramm für die Arbeitsweise bzw. Programme des System-ROMs 3 und des Anwendungs-ROMs 4 einer erfindungsgemäßen IC-Karte. Bei dieser Ausführungsform wird der Geheimcode 51 für die betreffende Karte in das EEPROM 5, bei dem es sich um einen nichtflüchtigen Speicher handelt, beim abschließenden Herstellungsschritt für die Fertigstellung der IC-Karte eingespeichert, wie es oben unter Bezugnahme auf die **Fig.** 1 erläutert wurde. Vor der Ausführung des Testprogramms wird ein von außen in die Karte eingegebener Geheimcode mit dem in der Karte bereits gespeicherten Geheimcode in Beziehung gesetzt oder verglichen. Wenn das Ergebnis positiv ist, wird das Speicher-Initialisierungs-Unterprogramm 36 durchgeführt und dann das Testprogramm 31.

Im EEPROM 5 wird getrennt vom Geheimcode 51 für die betreffende IC-Karte, mit dem ein von außen eingegebener Geheimcode vor der Ausführung des Testprogramms 41 zu vergleichen ist, der Speicherungs-Verifizierungs-Code 52 eingeschrieben und gespeichert, der angibt, ob der Geheimcode 51 bereits in der Karte gespeichert worden ist oder nicht. Wie bei konventionellen Karten hat dieser Speicherungs-Verifizierungs-Code 52 ein Bitmuster, das weder mit den Anfangswerten im EEPROM 5 noch mit den verschiedenen anderen Bitmustern übereinstimmt, die später im EEPROM 5 gespeichert werden können. Wenn die IC-Karte während der Herstellung und vor dem Speichern des Geheimcodes 51 im EEPROM geprüft werden soll, wird das Speicherinitialisierungs-Unterprogramm 36 nicht ausgeführt, sondern gleich das Testprogramm.

Gemäß dem Flußdiagramm in **Fig.** 3 liest die CPU 1 eine Ausführungs-Startadresse für das Verzweigungsunterprogramm 32 aus einer vorgegebenen Adresse im System-ROM 3 aus, wenn dem Rückstellsignaleingang P3 ein Rückstellsignal zugeführt wird, und die Durchführung des Verzweigungsunterprogramms 32 wird von dieser Ausführungsstartadresse aus begonnen. Wenn ein Kommando, das Testprogramm 31 durchzuführen, von außen über den I/O-Anschluß P5 zugeführt wird, veranlaßt das Verzweigungsunterprogramm 32 die CPU 1, das Speicherungs-Verifizierungs-Unterprogramm 34 durchzuführen. Das Speicherungs-Verifizierungs-Unterprogramm 34 stellt aufgrund des Speicherungs-Verifizierungs-Code 52 im EEPROM 5 fest, ob der Geheimcode 51 bereits im EEPROM 5 gespeichert worden ist. Wenn der Geheimcode 51 bereits gespeichert wurde, wird das Geheimcode-Verifizierungs-Unterprogramm 35 durchgeführt. Wenn er noch nicht gespeichert worden ist, wird der Geheimcodevergleich nicht durchgeführt, sondern sofort das Testprogramm

BNSDOCID: <DE___4100151A1_I >

31 ausgeführt.

Im Geheimcode-Verifizierungs-Unterprogramm 35 wird der über den I/O-Anschluß P5 eingegebene Geheimcode mit dem im EEPROM 5 gespeicherten Geheimcode verglichen und bei Übereinstimmung wird das Speicher-Initialisierungs-Unterprogramm 36 ausgeführt, um das EEPROM 5 zu initialisieren, wodurch verhindert wird, daß persönliche, den Karteninhaber betreffende Daten, die im EEPROM 5 gespeichert sind, herausgelesen werden können.

Wenn dem I/O-Anschluß P5 von außen kein Kommando zur Durchführung des Testprogramms zugeführt wird, führt die CPU 1 das Anwendungsprogramm 41 durch.

Bei der erfindungsgemäßen IC-Karte kann das Testprogramm ohne Initialisierung des EEPROMs 5 durchgeführt werden, wenn im EEPROM 5 der Karte noch kein spezieller Geheimcode fur die betreffende Karte gespeichert worden ist. Wenn jedoch der Geheimcode bereits im EEPROM 5 gespeichert worden ist, wird das EEPROM 5 durch das Speicher-Initialisierungs-Unterprogramm 36 initialisiert. Wenn also das Testprogramm für eine solche Karte absichtlich oder zufällig durchgeführt wird, wird ein Herauslesen von persönlichen Daten, die den Inhaber der Karte betreffen, verhindert. Während der Herstellung der IC-Karte ist der Geheimcode für die betreffende Karte noch nicht gespeichert und es erfolgt daher nie eine Initialisierung des EEPROMs 5. Bei der erfindungsgemäßen Karte können daher Prüfungen der verschiedenen Einrichtungen der Karten, einschließlich des EEPROMs 5, vor der Auslieferung der IC-Karten durchgeführt werden. Es ist also eine vollständige Prüfung der IC-Karten durchführbar.

Die IC-Karte mit einem in ihr enthaltenen Produkt-Testprogramm enthält also einen Lesespeicher. Dieser Lesespeicher speichert verschiedene Unterprogramme und ist so ausgebildet, daß wenn ein der betreffenden IC-Karte individuell zugeordneter Geheimcode bereits in einem nichtflüchtigen Speicher der IC-Karte gespeichert worden ist, ein von außen eingegebener Geheimcode mit dem gespeicherten Geheimcode verglichen wird und wenn der Vergleich positiv ausfällt, wird der nichtflüchtige Speicher initialisiert. Das Testprogramm kann erst ausgeführt werden, nachdem die Initialisierung fertig ist. Ein Zugriff auf andere Speicherinhalte ist dadurch nicht möglich.

Patentansprüche

1. IC-Karte, welche ein Testprogamm zu ihrer Prüfung enthält, mit
einer bespeicherbaren, nichtflüchtigen Speicheranordnung, in der ein der betreffenden IC-Karte individuell zugeordneter Geheimcode sowie ein Speicherungs-Verifizierungs-Code zur Verifizierung, daß der Geheimcode in die Speicheranordnung eingespeichert worden ist, eingeschrieben und gespeichert sind;
einer ersten Lesespeicheranordnung zum Speichern eines Anwendungsprogrammes für verschiedene Funktionen, die der IC-Karte zugeordnet sind;
einer zur Speicherung des Testprogramms dienenden zweiten Lesespeicheranordnung, die außerdem ein Verzweigungsunterprogramm zur Feststellung, ob das Testprogramm oder das Anwendungsprogramm durchzuführen ist, ein Speicherungs-Verifizierungs-Unterprogramm, das wenn das Testprogramm durchzuführen ist, aufgrund des Speicherungs-Verifizierungs-Code in der nichtflüchtigen Speicheranordnung feststellt, ob der Geheimcode bereits in der nichtflüchtigen Speicheranordnung gespeichert worden ist, und eine sofortige der Durchführung des Testprogramms ermöglicht, wenn der Geheimcode noch nicht gespeichert worden ist, ein Geheimcode-Verifizierungs-Unterprogramm zum Vergleichen eines von außen eingegebenen Geheimcodes mit dem gespeicherten Geheimcode, wenn das Speicherungs-Verifizierungs-Unterprogramm festgestellt hat, daß der Geheimcode bereits in die nichtflüchtige Speicheranordnung eingeschrieben worden und in dieser gespeichert ist, und ein Initialisierungs-Unterprogramm, welches die bespeicherbare, nichtflüchtige Speicheranordnung nur dann initialisiert, wenn der von außen eingegebene Geheimcode mit dem in der nichtflüchtigen Speicheranordnung gespeicherten Geheimcode übereinstimmt und nach der Vervollständigung der Initialisierung die Durchführung des Testprogramms ermöglicht, speichert;
eine Steueranordnung zur Durchführung und Steuerung der jeweiligen Programme;
eine Eingangs-Ausgangs-Steueranordnung zum Steuern der Signaleingabe in die und Signalausgabe von der IC-Karte von bzw. in eine außerhalb der IC-Karte befindliche Einrichtung; und
einem System-Bus zur Signalübertragung zwischen den verschiedenen Anordnungen.

2. IC-Karte nach Anspruch 1, dadurch gekennzeichnet, daß die bespeicherbare, nichtflüchtige Speicheranordnung ein elektrisch löschbares, programmierbares ROM ist.

3. IC-Karte nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Geheimcode in die beschreibbare, nichtflüchtige Speicheranordnung während der abschließenden Stufe des Herstellungsprozesses eingespeichert wird.

Hierzu 3 Seite(n) Zeichnungen

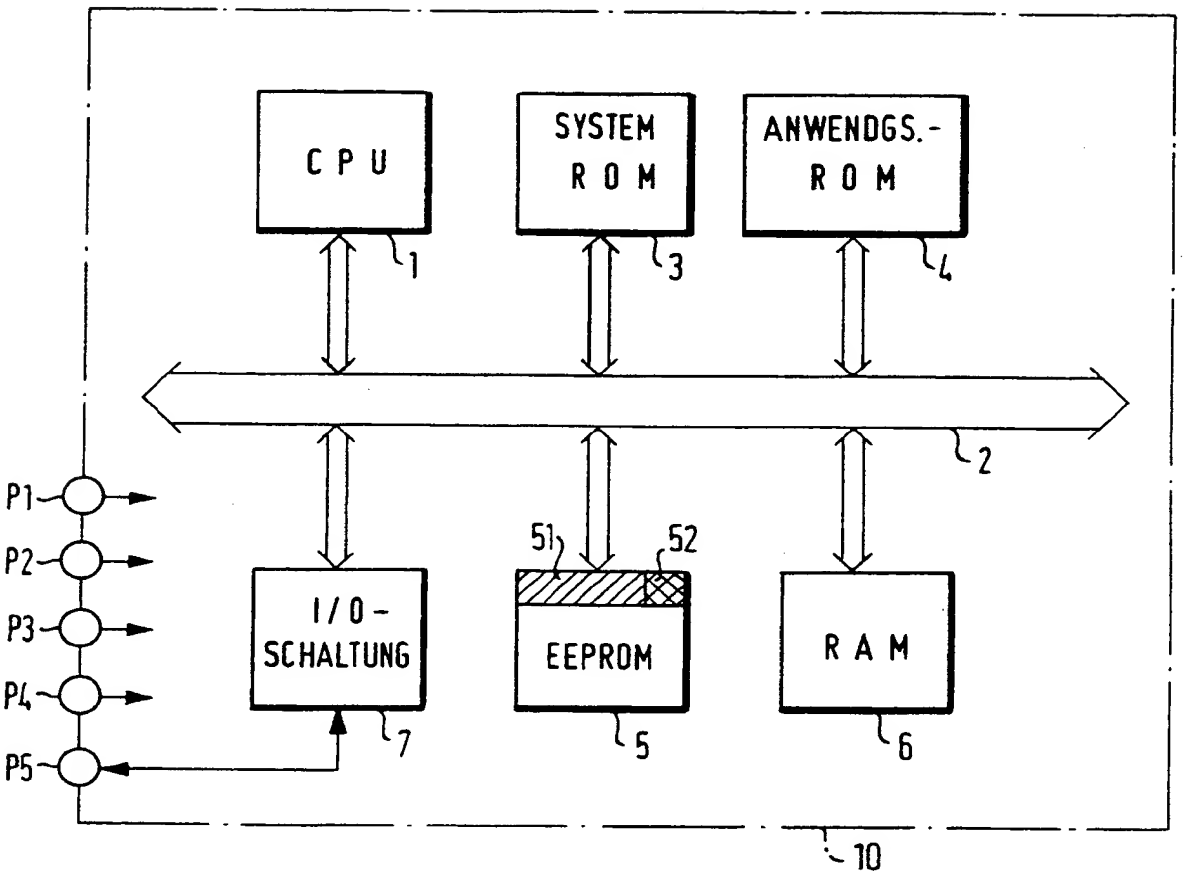
BNSDOCID: <DE 4100151A1 | >

— Leerseite —

BNSDOCID: <DE __ 4100151A1_I >

Nummer: DE 41 00 151 A1
Int. Cl.[5]: G 07 F 7/12
Offenlegungstag: 19. Dezember 1991

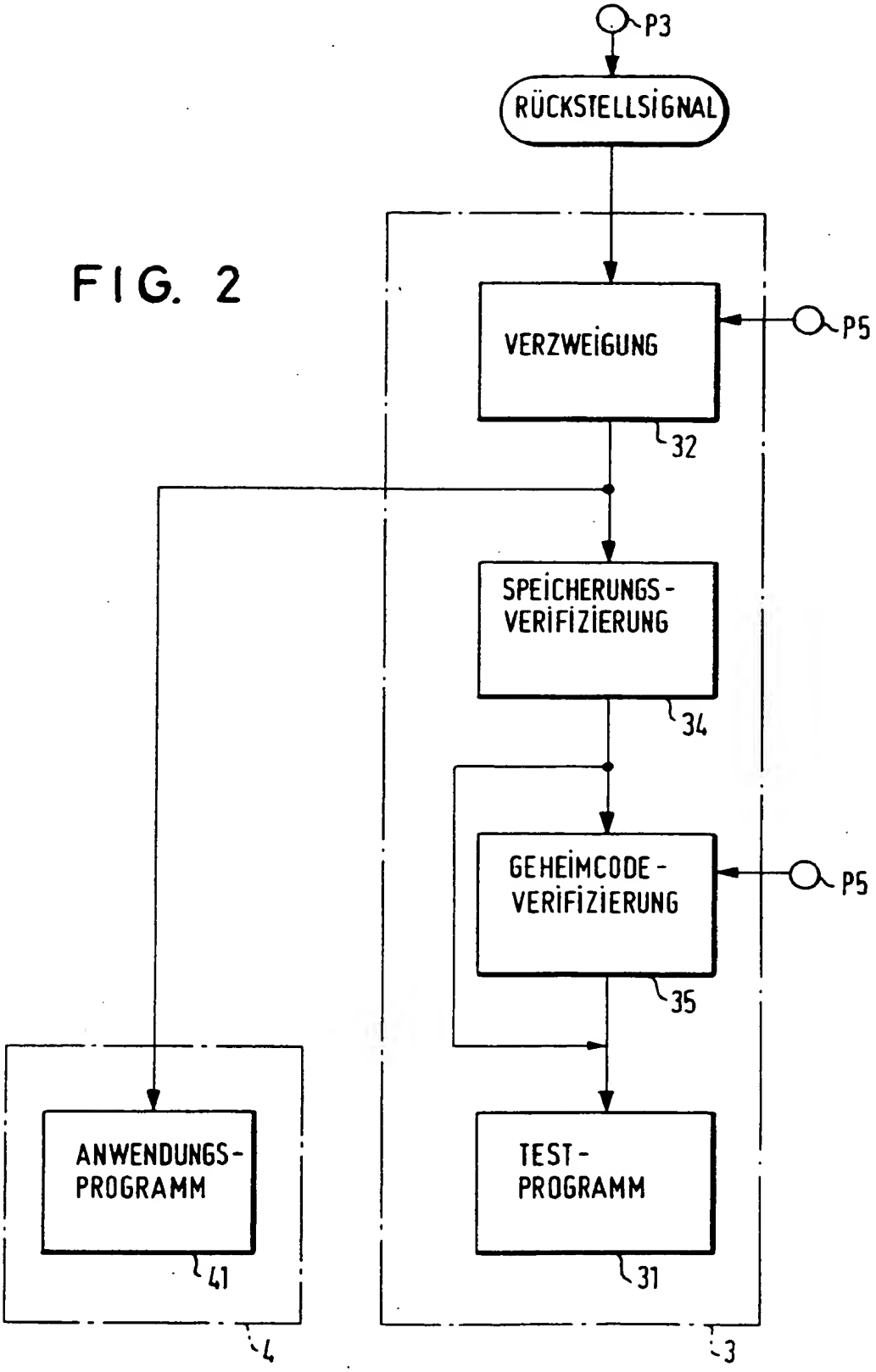
FIG. 1



BNSDOCID <DE 4100151A1 I >

Nummer: DE 41 00 151 A1
Int. Cl.[5]: G 07 F 7/12
Offenlegungstag: 19. Dezember 1991

FIG. 2



ENSDOCID: <DE___4100151A1_I_>

Nummer: DE 41 00 151 A1
Int. Cl.[5]: G 07 F 7/12
Offenlegungstag: 19. Dezember 1991

FIG. 3